006279/25-00.323

PODER JUDICIÁRIO
**SUPERIOR TRIBUNAL MILITAR**
PRSTM*/SECSTM/DITIN/CIBER

# ESTUDO TÉCNICO PRELIMINAR - TIC

# AQUISIÇÃO DE SOLUÇÃO DE VIDEOCONFERÊNCIA

Histórico de Revisões

| Data | Versão | Descrição | Autor |
|---|---|---|---|
| 17/03/2025 | 1.0 | Versão Inicial | Equipe de Planejamento da Contratação |

## ESTUDO TÉCNICO PRELIMINAR

### INTRODUÇÃO

O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Contratação TI DOD - STM/CJM 4234272, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

**Referência:** **Resolução CNJ Nº 468/2020** e **Lei n. 14.133, de 1º de abril de 2021**

### 1 – DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

#### 1.1 - DESCRIÇÃO DA NECESSIDADE

##### 1.1.1 – Descrição do Objeto Pretendido

Contratação de serviço de conteúdo na modalidade “Software as a Service” (SaaS) para treinamento usuários de TIC, por meio do acesso à plataforma online, especializada na oferta de conteúdos de capacitação e conscientização em Segurança da Informação.

##### 1.1.2 – Necessidade de Negócio

1.1.2.1 - Em diversos eventos, entre eles as capacitações técnicas, fóruns, congressos e seminários; fica nem estabelecido entre os participantes que um elevado percentual de incidentes tem origem nas pessoas, sendo, em muitos casos definido aos usuários de TI o termo "o elo mais fraco quando falamos em segurança cibernética".

1.1.2.2 - A ausência de cultura e a consequente falha na adoção de comportamentos preventivos faz com que os usuários se tornem a ponto de partida para os criminosos explorarem táticas de apropriação de credenciais de acesso ou de instalação de programas maliciosos que visam, como objetivo final, a invasão de rede, roubo de informações valiosas e causarem grandes prejuízos financeiros e de imagem às instituições.

1.1.2.3 - Treinar e conscientizar pessoas é primordial para o fortalecimento da segurança da infraestrutura tecnológica e dos dados pessoais e, não por acaso, está prevista na Resolução Nº 396 de 07/06/2021 do Conselho Nacional de Justiça (CNJ) a adoção deste tipo de ação, conforme descrito no item III do Art 17. que assim descreveu: "*.... III – elaborar e implementar programas sobre segurança da informação destinados à conscientização e à capacitação dos servidores do Poder Judiciário;...*"

1.1.2.4 - Entre outras ações, destacamos que em 2024 foi aprovado a instrutoria interna com o objetivo de se estabelecer uma capacitação básica para todos os usuários da JMU, que avança em sua última etapa neste primeiro semestre de 2025, todavia este processo de capacitação pode se comparar a uma vacina imunizante, onde, em um primeiro momento, as pessoas se apropriam do conhecimento e adotam comportamento preventivos, mas com o passar dos meses é natural que, gradativamente, as prevenções, por parte dos usuários treinados, sejam diminuídas, o relaxamento aumente e os riscos se potencializem.

1.1.2.5 - Diante do apresentado, tornar a capacitação de usuários um **programa contínuo** é uma necessidade, inclusive, prevista na Política de educação e cultura em segurança cibernética do Poder Judiciário, instituída pelo Conselho Nacional de Justiça (CNJ), que descreveu no item 2.1.3: "*...Cada órgão do Poder Judiciário deverá estabelecer uma carga horária mínima de capacitação não superior a 1 (um) ano...*".

Fonte: https://www.cnj.jus.br/wp-content/uploads/2021/03/AnexoVIIManualReferenciaPoliticaDeEducacaoCulturaSegurancaInformacaoRevisado-REV.docx.pdf

1.1.2.6 - Destacamos, também, o Ato Normativo Nº 742 que instituiu, no âmbito da Justiça Militar da União, a Política de Capacitação e Fomento da Cultura da Segurança Cibernética, estabelecendo responsabilidades para esta área especializada em segurança cibernética da Diretoria de Tecnologia da Informação e estabelece objetivos para o tema estabelecido.

1.1.2.7 - Por fim, há de se ressaltar a presente contratação esta estabelecida no escopo do Projeto Estratégico da Justiça Militar da União de Segurança da Informação, conforme se vê na Proposta de Abertura de Projeto SEI 3254771.

1.1.2.8 - Pelo exposto, a presente contratação se faz necessária e de extrema relevância não somente para mitigar riscos operacionais e técnicos, mas também para estabelecer conformidade com os normativos vigentes.

#### 1.2 – REQUISITOS DA CONTRATAÇÃO

##### 1.2.1 - Requisitos de Licenciamento para Solução de Software

1.2.1.1 - Para registro neste documento técnico, define-se como “Software como Serviço” (Software as a Service – SaaS).

1.2.1.2 - As soluções componentes podem ser acessadas por vários dispositivos, utilizando navegador web.

1.2.1.3 - A CONTRATANTE não gerencia nem controla a infraestrutura em nuvem que suporta a solução contratada, nem os componentes das soluções em software contratados.

1.2.1.4 - A CONTRATADA é responsável por manutenções e atualizações da solução, segurança, armazenamento, backup e demais recursos necessários ao funcionamento da solução.

1.2.1.5 - A CONTRATADA disponibilizará licenças de direito de uso dos componentes da Solução de Software - Software como Serviço (Software as a Service – SaaS) que deverá cumprir os REQUISITOS RELACIONADOS AO NEGÓCIO.

1.2.1.6 - A CONTRATADA se responsabilizará pela, manutenção e atualizações corretivas e evolutivas da Solução implantada.

## 1.3 – REQUISITOS RELACIONADOS AO NEGÓCIO

### 1.3.1 - Requisito principal do objeto

1.3.1.1 - A ferramenta deve ter como objeto a prestação de serviço, na modalidade “Software as a Service” (SaaS), acessada por meio do acesso à plataforma online, especializada na oferta de conteúdos de capacitação e conscientização em Segurança da Informação.

### 1.3.2 - Requisitos Básicos

1.3.2.1 - Disponibilizar ampla biblioteca de conteúdos de segurança da informação em língua portuguesa.

1.3.2.2 - Entregar conhecimento com uso de recursos interativos, como vídeos, questionários rápidos, boletins/textos informativos e outros meios adicionais.

1.3.2.3 - Possibilitar a inclusão de conteúdos educativos produzidos pela própria Justiça Militar da União, visto que esta Corte já possui profissionais que foram destacados para a realização de instrutoria interna sobre o tema e podem, dentro da cultura organizacional existente, contribuir com materiais que sejam de grande relevância para o aprimoramento do tema entre os usuários de TIC.

1.3.2.4 - Permitir a execução de campanhas e simulações de treinamento automatizadas, em especial, simulações de phishing (mensagens eletrônicas que são armadilhas para roubar dados e inserir vírus na rede).

1.3.2.5 - Permitir o carregamento de políticas e normas de segurança da Justiça Militar da União, podendo ser destacado o documento denominado "Termo de Responsabilidade e Custódia de Ativos e Recursos de TIC", que todo usuário deve ler, analisar a aceitar para que se homologue a concessão de credenciais de acesso aos meios tecnológicos.

1.3.2.6 - Permitir acompanhamento da evolução da maturidade dos usuários e da instituição em relação à Segurança da Informação.

1.3.2.7 - Permitir a gestão completa de treinamento executado pelos usuários de TIC por meio da ferramenta.

1.3.2.8 - Permitir integração com a base de dados de usuários da instituição.

1.3.2.9 - Permitir a automatização de tarefas, diminuindo a carga de trabalho que recaem sobre os recursos humanos de TIC da JMU, como por exemplo a atribuição automática de treinamentos e agendamento de campanhas de phishing.

1.3.2.10 - A plataforma de treinamento deve estar disponível no período de 24h x 7d para os usuários, durante toda a vigência da contratação.

### 1.3.3 - Requisitos de Ambiente, Culturais e Sociais

1.3.3.1 - Deve possuir conteúdo acessível à deficientes auditivos e visuais.

1.3.3.2 - Permitir a inclusão da identidade visual da instituição nas campanhas e treinamentos.

1.3.3.3 - Ambiente da plataforma deve ser disponibilizado totalmente em português.

### 1.3.4 - Requisitos de Segurança da Informação

1.3.4.1. - A CONTRATADA deverá submeter-se aos procedimentos contidos nas normas de segurança cibernética da JMU em todos os eventos em que for necessária a presença de seus prepostos e/ou funcionários nas dependências do órgão.

1.3.4.2. - A CONTRATADA deverá obedecer aos procedimentos operacionais de segurança da informação adotados pelo CONTRATANTE.

1.3.4.3. - A CONTRATADA não pode obter, capturar, copiar ou transferir qualquer tipo informação de propriedade da JMU sem autorização do CONTRATANTE.

1.3.4.4. - A CONTRATADA não poderá se utilizar da presente contratação para obter qualquer acesso não autorizado às informações de propriedade do CONTRATANTE.

1.3.4.5. - As informações a que a CONTRATADA terá acesso deverão ser utilizadas somente nos processos envolvidos para execução do objeto contratado.

1.3.4.6. - A CONTRATADA deverá informar imediatamente ao Fiscal Técnico do Contrato qualquer violação das regras de sigilo ora estabelecidas que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo, bem como de seus empregados, prepostos e prestadores de serviço.

1.3.4.7. - Após a assinatura do contrato, por meio de seu representante, também será necessária a assinatura do **Termo de Sigilo e Confidencialidade**, por meio do qual a CONTRATADA se responsabilizará pela manutenção de sigilo e confidencialidade das informações a que possa ter acesso em decorrência da contratação. O termo visa assegurar que a CONTRATADA manterá sigilo, sob pena de responsabilidade civil, penal e administrativa acerca de informações consideradas como de interesse restrito ou confidencial, e não podem ser de conhecimento de terceiros.

1.3.4.8. - O **Termo de Sigilo e Confidencialidade** deve conter ainda cláusulas específicas que obriguem e estabeleçam prazos para que a contratada, após o término do contrato, elimine todo e qualquer dado pessoal da contratante na plataforma.

1.3.4.9. - O **Termo de Sigilo e Confidencialidade** deve conter, explicitamente, a garantia de segurança, sigilo e confidencialidade das informações dos usuários da JMU carregadas na plataforma.

1.3.4.10. - Não haverá compartilhamento de dados pessoais ou dados pessoais sensíveis com a CONTRATADA por parte da CONTRATANTE.

**1.3.5 Requisitos de Garantia, Suporte Técnico e Manutenção**

Para garantir a qualidade e a continuidade dos serviços prestados na contratação da solução em tela, seguem os principais requisitos de garantia contratual, suporte e manutenção:

1.3.5.1 - Garantia e Conformidade técnica: A CONTRATADA deve garantir de que todos os componentes da solução atendem aos requisitos estabelecidos, bem como à especificação técnica contida no Termo de Referência.

1.3.5.2 - Desempenho e Capacidade: A solução deverá possuir desempenho suficiente para atender ao volume de usuários, dados e transações demandados pela unidades da JMU, sem degradação da performance até o limite de utilização da capacidade máxima dos serviços contratados.

1.3.5.3 - Manutenção e Atualizações:

1.3.5.3.1 - A CONTRATADA deverá providenciar a configuração, atualização e ativação de todos os serviços necessários ao bom funcionamento da solução durante toda a vigência da contratação.

1.3.5.3.2 - A solução deve estar atualizada com novas versões, corretivas e evolutivas, lançadas pelo fabricante durante o período contratual, que devem estar disponíveis ao CONTRATANTE em até 60 (sessenta) dias após o lançamento.

1.3.5.3.3 - A aplicação de novas versões, atualizações e correções não deve gerar indisponibilidade ou janela de manutenção ao CONTRATANTE.

1.3.5.4 - Suporte Técnico:

1.3.5.4.1 - Durante o período de garantia, a CONTRATADA deverá oferecer suporte técnico referente a funcionalidades, configuração, características técnicas ou softwares referentes ao serviço fornecido.

1.3.5.4.2 - O suporte técnico deverá ser prestado por técnicos qualificados pela fornecedora da solução. O profissional deve estar acessível no período 8hx5d, dias úteis.

1.3.5.4.3 - O acionamento do suporte será mediante chamado técnico realizado pela CONTRATANTE, na pessoa dos gestores da plataforma ou servidor(es) delegados por um ou mais gestor da plataforma.

1.3.5.4.4 - O suporte poderá ser ofertado por e-mail, telefone ou sistema eletrônico, sempre considerando a solução do problema relatado pela CONTRATANTE.

**1.4. NECESSIDADES TECNOLÓGICAS**

1.4.1 - Acesso ilimitado à biblioteca com, no mínimo, 300 (trezentos) itens de conteúdo de segurança da informação em português, ou em língua estrangeira com legendas em português.

1.4.1.1 - Plataforma deve estar em conformidade com o padrão WCAG (versão 2 ou superior), para atender as necessidades de usuários com deficiências visuais, auditivas, motoras e cognitivas.

1.4.1.2 - Desejável que possua conteúdo específico voltado a LGPD Brasileira.

1.4.2 - Entregar conhecimento através de conteúdos tais como: vídeos, questionários rápidos, boletins/textos informativos, artes (posteres) e assessments (avaliações).

1.4.3 - Prover gerenciamento de usuários e cursos, permitindo:

1.4.3.1 - Seleção de módulos de treinamento para grupo de usuários.

1.4.3.2 - Atribuição automática de treinamentos para novos usuários.

1.4.3.3 - Disparo automático de e-mails de lembrete para usuários com treinamentos pendentes.

1.4.3.4 - Carga de usuários por meio de arquivo .CSV.

1.4.3.5 - Integração com o AD (Active Directory) da contratante.

1.4.3.6 - Inativação de usuários sem perda do histórico de dados.

1.4.3.7 - Permitir que uma licença de acesso utilizada por um usuário desligado da contratante possa ser aplicada a um novo usuário, durante o período remanescente do contrato. Neste caso, não é necessária a manutenção do histórico do usuário antigo.

1.4.4 - Permitir inserir a identidade visual da contratante nas campanhas e nas mensagens dirigidas aos usuários.

1.4.5 - Permitir a carga de conteúdos próprios de treinamento em segurança da Informação da contratante, em vídeo, no formato PDF ou no padrão SCORM.

1.4.5.1 - Todas as funcionalidades de gestão disponíveis para os conteúdos nativos devem poder ser aplicadas aos conteúdos próprios da contratante.

1.4.6 - Permitir a carga e o aceite de políticas e normas de segurança da informação da contratante.

1.4.7 - Prover ambiente de gestão para acompanhamento online de progressão e desempenho dos usuários.

1.4.8 - Disponibilizar detalhes sobre a porcentagem de inscrições, cursos iniciados, incompletos, concluídos e conhecimento da política de segurança e normas.

1.4.9 - Prover ambiente de gestão que possibilite a criação de grupos de usuários com base em comportamento frente às simulações e treinamentos realizados.

1.4.10 - Disponibilizar relatórios executivos e de gestão sobre as campanhas e resultados de treinamentos.

1.4.11 - Permitir a emissão de certificados para os treinamentos.

1.4.12 - Prover APIs de relatórios que permitam personalizar os documentos, integrando-os a outros sistemas de negócios para apresentar os dados a partir da plataforma.

1.4.13 - Disponibilizar perfis de acesso para gestão de campanhas e treinamentos (desejável também perfil para auditoria, porém não obrigatório).

1.4.14 - Possibilitar a autenticação em dois fatores para usuários e administradores.

1.4.15 - Possibilitar a criação de campanhas simuladas de phishing, a fim de avaliar o comportamento dos usuários.

1.4.15.1 - Permitir criação de número ilimitado de campanhas durante a vigência do contrato.

1.4.15.2 - Disponibilizar pelo menos 50 (cinquenta) modelos de campanhas em português e permitir a personalização dos modelos diretamente pela contratante.

1.4.15.3 - Manter histórico por usuário e por campanha.

1.4.15.4. - Permitir que os usuários seja testados e instruídos instantaneamente sobre os indicativos fraudulentos da simulação.

1.4.15.5 - Possibilitar a criação automatizada de um programa personalizado em segurança da informação ou fazer a recomendação automática de treinamentos, considerando, no mínimo, o nível de risco em segurança da informação dos usuários.

1.4.16 - Apresentar painel gerencial com indicador de nível de risco em segurança da informação para cada usuário e para a instituição. O nível de risco deve ser medido considerando-se pelo menos dois fatores: participação em treinamentos e avaliação nos testes de phishing.

1.4.17 - Disponibilizar ambiente operacional para alunos e administradores totalmente em língua portuguesa (pt-br).

1.4.18 - Para evitar dependência tecnológica, a plataforma deve prover APIs que permitam a exportação contínua de todas as informações gerenciais da plataforma de conscientização para base de dados própria da contratante. Informações como evolução da maturidade dos usuários (nível de risco), cursos efetuados, certificados, resultados de testes de phishing, etc, devem ser passíveis de exportação através de APIs.

**1.5. IMPLANTAÇÃO E SUPORTE**

1.5.1 - PREMISSAS

1.5.1.1 - A contratada deve disponibilizar, durante todo período contratual, um gerente de contas para apoiar e orientar a contratante no uso da plataforma. O gerente de conta tem como atribuições:

1.5.1.1.1 - Acompanhar o projeto (programa de conscientização).

1.5.1.1.2 - Esclarecer dúvidas.

1.5.1.1.3 - Sugerir proativamente novos caminhos para o programa.

1.5.1.1.4 - Ser ponte com o suporte técnico.

1.5.1.1.5 - Configurar a conta e fazer a integração com a infraestrutura da contratante (onboarding).

1.5.1.2 - A contratada deve efetuar, a partir das informações fornecidas pela contratante, a implantação da solução (onboarding), tarefa que consiste na configuração e integração da infraestrutura tecnológica da contratante com a plataforma. A tarefa envolve, sempre que aplicável, no mínimo:

1.5.1.2.1 - Inclusão das informações dos servidores da contratada em listas de permissão (whitelisting) da contratante.

1.5.1.2.2 - Configuração da integração com Active Directory e ADFS.

1.5.1.2.3 - Carregamento dos usuários (extraídos do AD) e classificação em grupos.

1.5.1.2.4 - Habilitação de Duplo Fator de Autenticação.

1.5.1.3 - Deve ser agendada no mínimo 1 (uma) reunião por videoconferência entre o gerente de contas e os administradores da contratante para passagem de conhecimento, durante o período de onboarding.

1.5.1.3.1 - A passagem de conhecimento deve envolver, no mínimo: Melhores práticas para implantação; Forma de Acesso dos usuários e download de conteúdos; Criação de grupos inteligentes; Atribuição de treinamentos a grupos de usuários; Carga de conteúdos da contratante; Criação e automatização de campanhas de phishing; Criação de roles (papeis) de segurança; Carga, inativação e exclusão de usuários; Personalização de identidade visual; Emissão e extração de relatórios.

1.5.1.3.2 - Toda instrução e passagem de conhecimento é aberta ao quantitativo de profissionais necessários para gestão da plataforma, a critério da contratante.

1.5.1.3.3- A contratante poderá ainda, a seu critério, solicitar a inclusão de qualquer outro tema relacionado às especificações constantes neste termo de referência.

1.5.1.3.4 - A critério da contratante, podem ser solicitadas outras reuniões por videoconferência com o gerente de contas durante a vigência do contrato.

1.5.1.3.5 - Toda instrução e passagem de conhecimento é aberta ao quantitativo de profissionais necessários para gestão da plataforma, a critério da contratante.

1.5.1.3.6 - A contratante poderá ainda, a seu critério, solicitar a inclusão de qualquer outro tema relacionado às especificações constantes neste documento.

1.5.1.4 - A critério da contratante, podem ser solicitadas outras reuniões por videoconferência com o gerente de contas durante a vigência do contrato.

1.5.2 - DOS PRAZOS INICAIS

| ITEM | TAREFA | DESCRIÇÃO | EXECUTOR | Prazo |
|---|---|---|---|---|

| | | | | **Máximo**<br>**(Dias úteis)** |
|---|---|---|---|---|
| 1 | Contrato Firmado | Assinatura do Contrato | CONTRATANTE E CONTRATADA | Dia "D" |
| 2 | Reunião de Alinhamento | Reunião - Alinhamento do Programa e Apresentação de Funcionalidades da Plataforma | CONTRATANTE E CONTRATADA | D + 5 |
| 3 | Fase 1 da Implantação | Entrega da fase 1 - Liberação das Licenças de Acesso à Plataforma. | CONTRATADA | D + 5 |
| 4 | Fase 1 da Implantada | Emitir termo de recebimento provisório por meio de processo SEI | CONTRATANTE | Em até 5 dias corridos da Entrega da fase 1<br>DIA "R1" |
| 5 | Fase 2 da Implantação | Entrega da Fase 2 - Configurar a conta, fazer carga de Usuários e a integração com a infra da contratante (onboardind)<br>Passagem de Conhecimento | CONTRATANTE E CONTRATADA | R1 + 20 |
| 6 | Fase 2 Implantada | Elaborar documento de Termo de recebimento Definitivo, caso a solução tenha atendido os critérios estabelecidos em edital para esta etapa | CONTRATANTE | Em até 10 dias corridos<br>da Entrega da fase 2<br>DIA R2 |
| 7 | Definição de Prazos | Vigência das Licenças de Acesso | CONTRATANTE E CONTRATADA | R2 + 36 MESES |

**1.6. DEMAIS REQUISITOS NECESSÁRIOS E SUFICIENTES PARA A ESCOLHA DA SOLUÇÃO**

São requisitos necessários e suficientes para a escolha da solução os requisitos a seguir:

1.6.1 - Requisitos legais. A contratação de Solução de Tecnologia da Informação deverá respeitar as seguintes normas:

1.6.1.1 - **Lei nº 14.133, de 1º de abril de 2021.** que institui normas para licitações e contratos da Administração Pública.

1.6.1.2 - **Lei no 13.709, de 14 de agosto de 2018,** que institui a Lei Geral de Proteção de Dados Pessoais (LGPD).

1.6.1.3 - **Resolução CNJ nº 468 de 15 de julho de 2022**, que dispõe sobre diretrizes para as contratações de Solução de TIC no poder judiciário.

1.6.1.4 - **Lei de Acesso à Informação, nº 12.527 de novembro de 2011.**

1.6.1.5 - **Resolução 350 -** (3727711) **-** que institui a Política de Segurança Cibernética da JMU.

1.6.2 - Qualificação Técnico Financeira

1.6.2.1 - Apresentar atestado de capacidade técnica, emitido por pessoa jurídica de direito público ou privado, que comprove ter a licitante executado, satisfatoriamente, o fornecimento de no mínimo 750 (setecentos e cinquenta) licenças de acesso à plataforma de conscientização ofertada, quantidade que representa 50% da demanda da Justiça Militar da União.

1.6.2.1.1 - Será aceito o somatório de atestados de períodos concomitantes para certificar que todo o quantitativo indicado na cláusula anterior já tenha sido fornecido pela licitante.

1.6.2.2 - Apresentar, para fins de qualificação econômico-financeira, certidão negativa de feitos sobre falência, recuperação judicial ou recuperação extrajudicial, expedida pelo distribuidor da sede da licitante, que se encontre dentro do prazo de validade. Caso não haja prazo de validade especificado no documento, será considerado o prazo máximo de 30 (trinta) dias, contados da data de sua expedição.

1.6.3 - Análise da Dependência Tecnológica

1.6.3.1 - Em termos gerais, busca-se contratar uma plataforma com conteúdo de conscientização e treinamento para a Justiça Militar da União. Quanto a esse aspecto não há que se falar em dependência tecnológica. Funciona como qualquer outra plataforma de treinamento: os cursos ficam disponíveis somente durante a vigência contratual e, neste período, capacitações podem ser iniciadas e finalizadas, sem qualquer restrição. Após o término do contrato o acesso ao conteúdo não é mais permitido. No entanto, há que se considerar outros aspectos relacionados aos requisitos de negócio estabelecidos, que não implicam em uma dependência tecnológica propriamente dita, mas indicam a necessidade de alguns cuidados no que tange à gestão no término do contrato. São eles:

1.6.3.1.1 - Certificados de conclusão dos Cursos.

1.6.3.1.2 - Avaliação de maturidade em segurança dos usuários e da instituição.

1.6.3.1.3 - Conteúdos da contratante disponibilizados na plataforma.

1.6.3.1.4 - Aceite das normas de segurança da informação.

1.6.3.2 - Antes do término do contrato, a contratante deverá efetuar a exportação de todo o conteúdo, tais como: certificados, relatórios de nível de risco, cursos próprios inserido na plataforma e relação das normas com os respectivos aceites e providenciar uma nova forma de armazenamento e

gestão, ou com recursos tecnológicos próprios ou através de novos contratos. Está sendo exigido que a plataforma possua APIs internas que permitam que essa exportação seja feita ao longo do contrato.

## 2 – ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

2.1 - Estimativa da Demanda

2.1.1 - A solução pretendida não existe na JMU;

2.1.2 - Para a composição da estimativa da demanda, foram utilizados como referência para o cálculo total, o somatório dos números contidos em 3(três) informações relevantes, a saber:

2.1.2.1 - o volume total de contas de e-mail ativas, que hoje está estabelecido em **1.282 (um mil duzentos e oitenta e dois)** registros.

2.1.2.2 - a estimativa do aumento de servidores nos próximos meses, em razão da aprovação da Lei 14.741/23, combinado com o Parágrafo 1º e 7º do Art. 5 da Lei 11.416 de 15/12/2006 que confere um valor de aproximadamente **250 (duzentas e cinquenta)** novas nomeações.

2.1.2.3 - estimativa de **200 (duzentos)** estagiários e terceirizados que, atualmente lotados na JMU, não dispõem de conta de e-mail institucional.

2.1.3 - Com base nas análise realizadas durante os estudos técnicos, sobretudo considerando as varáveis acima descritas, foi estipulado o quantitativo de licenças necessárias e suficientes a serem adquiridas para a implantação do serviço de para treinamento usuários de TIC, por meio do acesso à plataforma online, especializada na oferta de conteúdos de capacitação e conscientização em Segurança da Informação, apresentado no **Quadro - Estimativa de Demanda**.

**Quadro - Estimativa de Demanda**

| LOTE ÚNICO | | |
|---|---|---|
| **ITEM** | **CATSER** | **QTD** |
| 01 | 27502 -Serviços de fornecimento de subscrição de licenças de acesso à plataforma em nuvem de capacitação e conscientização em segurança da informação fornecida como serviço (SaaS), com implantação e suporte inclusos | 1.732 |

## 3 – ANÁLISE DE SOLUÇÕES POSSÍVEIS

No contexto da análise de soluções possíveis, cabe destacar que este processo objetiva a implantação de um novo serviço no STM e em todas as Auditorias da JMU.

3.1 - Contratações Públicas Similares

3.1.1 - Foi efetuada pesquisa no painel de preços do governo federal (**https://paineldeprecos.planejamento.gov.br/analise-servicos**) e na ferramenta Banco de Preços Públicos (**https://www.gov.br/governodigital/pt-br/software-publico**) com o objetivo de identificar contratações similares efetuadas por órgãos públicos federais ou instituições públicas, foi constatado que a solução tem sido amplamente contratada pela Administração Pública, conforme quadro apresentado a seguir:

**Quadro - Levantamento de Contratações Públicas Similares**

| Órgão | Documento SEI de referência | Descrição | QTD MESES | Licenças | Valor Total da Contratação | Valor Unitário da Licença Por Ano | Data de Aquisição |
|---|---|---|---|---|---|---|---|
| Tribunal de Justiça da Bahia | Comprovante - TJBA (4234840) | Contratação de uma empresa especializada no fornecimento de subscrição de licenças de acesso à plataforma de treinamento online\, especializada em oferta de conteúdos de capacitação e conscientização em segurança da informação\, com simulação de ataques de engenharia social na modalidade Software como Serviço ( Software as a Service SaaS ) para magistrados. servidores\, estagiários\, terceirizados ou qualquer outro usuário que utilizem os serviços de tecnologia do TJBA | 24 | 12.000 | **R$ 1.900.980,00** | **R$ 79,20** | 28/08/2024 |
| Superior Tribunal de Justiça - STJ | Comprovante - STJ (4234841) | Pregão Eletrônico - Registro de preço para fornecimento de licenciamento de uso da plataforma KnowBe4 para ações de conscientização em Segurança da Informação e Defesa Cibernética e em Lei Geral de Proteção de Dados brasileira no Superior Tribunal de Justiça - STJ., Pregão Eletrônico - Contratação de uma empresa especializada no fornecimento de subscrição de licenças de acesso à plataforma de treinamento online\, especializada em oferta de conteúdos de capacitação e conscientização em segurança da informação\, com simulação de ataques de engenharia social na modalidade Software como Serviço ( Software as a Service SaaS ) para magistrados. servidores\, estagiários\, terceirizados ou qualquer outro usuário que | 24 | 4.809 | **R$ 633.736,00** | **R$ 65,89** | 11/07/2024 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | utilizem os serviços de tecnologia do TJBA. | | | | | |
| TJMSP | Comprovante - TJMSP (4234842) | Licenciamento de Software de Videoconferência, incluindo garantia técnica, pelo período de 36 (trinta e seis) meses | 12 | 245 | **R$ 42.630,00** | **R$ 174,00** | 30/12/2024 |
| CEMIG | Comprovante - CEMIG (4234843) | | 12 | 9.000 | **R$ 345.000,00** | **R$ 38,33** | 28/01/2025 |

**3.2 Existência de Software Livre ou Software Público**

Não há solução deste tipo que atenda os requisitos funcionais e técnicos.

**3.3 Análise Comparativa das Soluções de Mercado.**

3.3.1 - Com base nos requisitos estabelecidos neste documento, buscou-se no mercado plataformas de capacitação em segurança da informação que fossem aderentes às necessidades, considerando:

3.3.1.1 - Fossem notoriamente reconhecidas nesse campo de atuação - conscientização em segurança da informação.
3.3.1.2 - Disponibilizassem biblioteca de conscientização e capacitação em português (em linguagem nativa ou legendado).
3.3.1.3 - Agregassem o recurso prático de treinamento dos usuários através de simulações de phishing, que é, hoje, a técnica de engenharia social mais usada por invasores contra os usuários de tecnologia da informação.
3.3.1.4 - Permitissem a integração de conteúdo da Justiça Militar da União, a exemplo de treinamentos de capacitação em andamento, bem como de normas e documentos institucionais.
3.3.1.5 - Trouxessem o indicador de evolução da maturidade dos usuários e da instituição durante a execução do programa.
3.3.1.6 - Disponibilizassem a gestão integrada de todos os recursos.

3.3.2 - Com base em estudos técnicos já realizado por outros Órgãos Públicos (Justiça Eleitoral e TJBA) as plataformas Hackers Rangers, Knowbe4 e Proofpoint, apresentam as seguintes características e diferenças entre si:

| Tema | Descrição | Hackers Rangers | Knowbe4 | Proofpoint |
|---|---|---|---|---|
| **Conteúdo Nativo** | Conteúdo em língua portuguesa ou legendado em português nacional (300 itens) | **NÃO (80)** | **SIM (486)** | **SIM (403)** |
| | Conteúdo LGPD Nacional | **SIM** | **SIM** | **SIM** |
| | Entregar conhecimento através de conteúdo, tais como: vídeos, games, quizzes, artes (pôsteres), assessments (avaliações) | **SIM** | **SIM** | **SIM** |
| | Plataforma/Conteúdo em conformidade com padrão WCAG (versão 2 ou superior) | **N/A** | **SIM** | **SIM** |
| **Conteúdo do Cliente** | Permite carga de treinamentos da contratante, incluindo os formatos de vídeo e SCORM (Moodle, plataforma de educação à distância utilizada na JMU - DIPES e ENAJUM) | **NÃO PERMITE SCORM** | **SIM** | **NÃO** |
| | Todas as funcionalidades da plataforma aplicáveis ao conteúdo nativo são aplicáveis ao conteúdo da contratante inserido na plataforma | **SIM** | **SIM** | **SIM** |
| **Implantação e Segurança** | Possuir integração com AD e carga de usuários por meio de arquivos csv | **SIM** | **SIM** | **SIM** |
| | Permitir duplo fator de autenticação para usuários e administradores | **NÃO** | **SIM** | **NÃO** |
| **Normas de Segurança** | Permite a inclusão dos normativos de segurança da contratante e o aceite pelos usuários, em formato PDF | **NÃO** | **SIM** | **NÃO** |
| **Automação** | Atribuição automática de treinamento para novos usuários | **NÃO** | **SIM** | **NÃO** |

| | | | | |
|---|---|---|---|---|
| | Criação automatizada de um programa personalizado em segurança da informação ou recomendação automática de treinamentos, considerando, no mínimo, o nível de risco em segurança da informação dos usuários; | **NÃO** | **SIM** | **NÃO** |
| | APIs que permitam a exportação contínua de todas as informações gerenciais da plataforma de conscientização para base de dados própria da contratante | **NÃO** | **SIM** | **SIM** |
| **Campanha de Phishing** | Disponibiliza pelo menos 50 modelos de campanhas em português e permitir a personalização dos modelos pela contratante | **SIM** | **SIM** | **SIM** |
| | Mantem histórico por usuários e por campanha | **SIM** | **SIM** | **SIM** |
| | Permite que os usuários sejam testados e instruídos instantaneamente sobre os indicativos fraudulentos da simulação | **SIM** | **SIM** | **SIM** |
| **Indicador de Maturidade em Segurança** | Possui indicador de nível de risco em segurança da informação para cada usuário e para a instituição, devendo ser medido considerando se pelo menos dois fatores: participação em treinamentos e avaliação nos testes de phishing. | **NÃO** | **SIM** | **NÃO** |
| **Linguagem da Plataforma** | Disponibilizar ambiente operacional para alunos e administradores totalmente em língua portuguesa (ptbr) | **SIM** | **SIM** | **NÃO** |

3.3.3 - Importante destacar que entre as plataformas analisas, a plataforma Knowbe4 foi a única que Permite carga de treinamentos da contratante, incluindo os formatos de vídeo e SCORM (Moodle, plataforma de educação à distância utilizada na JMU - DIPES e ENAJUM). Não obstante, é relevante informar que a JMU, em sua estrutura administrativa, possui Seções específicas que criam conteúdos de capacitações em vídeos, com investimentos públicos já realizados neste sentido.

3.3.4 - Da Plataforma/Conteúdo em conformidade com padrão WCAG (versão 2 ou superior)
Trata-se de exigência com objetivo de não excluir os servidores, estagiários e colaboradores da JMU que possuem deficiência visual, auditiva ou motora. É necessário que a solução contratada atenda a esse público, de modo que não sejam preteridos em relação aos servidores sem deficiência. A produção de conteúdo nesses padrões mostra que a plataforma está preocupada com inclusão digital. A exigência atende à resolução CNJ 401/2021, em especial o artigo segundo, quando cita a eliminação de barreiras tecnológicas: "*... A fim de promover a igualdade, deverão ser adotadas, com urgência, medidas apropriadas para eliminar e prevenir quaisquer barreiras urbanísticas ou arquitetônicas, de mobiliários, de acesso aos transportes, nas comunicações e na informação, atitudinais ou tecnológicas...*"

3.3.5 - Da Possibilidade da autenticação em dois fatores para usuários e administradores.
O duplo fator de autenticação é um mecanismo de segurança que cria um 2o nível de segurança, além do login e senha, para que os usuários e administradores tenham acesso aos dados na plataforma. No caso dessa contratação, uma invasão através do comprometimento do login e senha poderia dar acesso a informações valiosíssimas para um invasor. Ele teria acesso a, por exemplo:

3.3.5.1 - Quais os usuários menos treinados na JMU.
3.3.5.2 - Quais usuários mais falharam nos testes de engenharia social.
3.3.5.3 - Informações pessoais como nome, cpf, email e outras disponíveis na plataforma.

De posse dessas informações, o invasor poderia direcionar os ataques de engenharia social para esses usuários e ter sucesso em uma invasão à instituição. Assim, é imprescindível que essa exigência voltada à segurança seja mantida pela Administração.

3.3.6 - Do Indicador de Maturidade em Segurança da Informação.
O Acórdão TCU Plenário 3143/2021 determina a implantação de um programa permanente de conscientização. É fundamental que a solução proporcione uma forma efetiva de avaliar a evolução da maturidade do Órgão em Segurança, visando a definição dos caminhos a serem seguidos na condução do programa. Neste contexto, o indicador de evolução de maturidade é primordial. Os parâmetros mínimos para este indicador são relativamente simples e estão claramente descritos - treinamentos realizados e avaliação dos testes de phishing. Cabe acrescentar que a tarefa de efetuar cálculos manuais de maturidade a partir de
informações de centenas ou milhares de usuários (no caso de alguns tribunais), não é razoável. Conforme já abordado neste estudo, há necessidade de racionalizar a força de trabalho da Justiça Militar da União, que já é demasiadamente reduzida, voltando o esforço do corpo de servidores para tarefas fins que não são passíveis de automação.

3.3.7 - Das API's para exportação dos dados.
A própria redação do item já trás a justificativa de sua necessidade. A funcionalidade tem como objetivo evitar dependência tecnológica. A resolução CNJ no 182/2013, em seu Art 18, §3, III, a), 8) determina que o termo de referência deve prever mecanismos para minimizar a dependência técnica da contratada. As APIs permitem a exportação contínua de todas as informações gerenciais da plataforma de conscientização para a base de dados da própria contratante., tais como o nível de risco dos usuários, cursos efetuados, certificados, resultados de testes de phishing, etc.

3.3.8 - Da Atribuição automática de treinamentos para novos usuários e da Possibilidade da criação automatizada de um programa personalizado em segurança da informação ou fazer a recomendação automática de treinamentos, considerando, no mínimo, o nível de risco em segurança da informação dos usuários.

3.3.9 - Os itens de automação alinham-se com a necessidade de racionalização da força de trabalho da Justiça Militar da União, além de estabelecer padrões claros para o treinamento dos usuários, especialmente para aqueles que acabaram de ingressar no Órgão, sem qualquer conhecimento da cultura e do contexto de segurança da informação em seu novo ambiente de trabalho. A atribuição automática de um conjunto de treinamentos para os novos usuários permite um nivelamento mínimo inicial que fortalecerá a segurança da informação do órgão. A criação automática de programas personalizados com base no indicador de maturidade justifica-se pelos mesmos motivos: racionalização de recursos humanos e padronização do programa.

## 4 – INDICAÇÃO DA SOLUÇÃO DE TIC ESCOLHIDA

4.1 - Solução de mercado, comercial.

4.2 - Contratação de licenças de acesso à plataforma integrada de treinamento online, especializada em oferta de conteúdos de capacitação e conscientização em Segurança da Informação.

4.3 - A solução deverá estar aderente aos requisitos descritos neste documento.

## 5 - ANÁLISE COMPARATIVA DE CUSTOS

5.1 - Ao se analisar o **Quadro - Levantamento de Contratações Públicas Similares,** descrito no item 3.1 deste documento, fica evidenciado que **média dos valores contratados**, nos últimos meses, ficou em **R$ 89,36 (oitenta e nove reais e trinta e seis centavos) licença/ano.**

5.2 - A variação de valores também chama a atenção, visto que o custo mensal unitário de menor valor (licença/ano) ficou fixado em R$ 38,33 (trinta e oito reais e trinta e três centavos), já o maior em R$ 174,00 (cento e setenta e quatro reais), ou seja, aproximadamente 354% acima do menor valor.

5.3 - Também **há conhecimento desta equipe que o TRE-ES está desenvolvendo um projeto de aquisição, do mesmo objeto, que visa adquirir 34.467 licenças, a um custo unitário de R$ 35,49 (trinta e cinco reais e quarenta e nove centavos)**, valor da licença (por ano) menor que todos aqueles contratados nos últimos meses, devendo ser considerado que a proposta é para a solução mais completa de mercado. Acreditamos que a enorme redução de valor decorre do volume de licenças contratadas combinado com o prazo contratual a ser estabelecido, promovendo, *s.m.j.*, **grande vantagem à administração pública**.

## 6 – ADERÊNCIA AOS REQUISITOS

6.1 - A solução que mais se adequa aos requisitos necessários, dentro daquelas estudadas e enunciadas no quadro demonstrativo contido no item 3.3.2. deste documento é a KnowBe4, a mesma ferramenta contida na proposta comercial enviada ao **TRE-ES a um valor unitário de R$ 35,49 (trinta e cinco reais e quarenta e nove centavos)**, valor da licença (por ano) menor que todos aqueles contratados nos últimos meses por Órgãos Públicos.

## 7 – ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

7.1. Com base nas pesquisas realizadas e apresentadas no item 3.1 deste documento e das considerações apresentadas nos itens 5.1, 5.2 e 5.3; há 02(dois) cenários a ser considerados no valor total previsto para a aquisição, conforme se vê no quadro demonstrativo abaixo:

**Quadro 11** - Estimativas de Custos

| **LOTE ÚNICO** | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Item** | **CATSER** | **Descrição** | **unidade** | **QTD** | **Parâmetro Adotado** | **Valor Unitário por ano<br>Por LIcença** | **Valor Total para todas as Licenças<br>Anual<br>12 (doze) meses** | **Valor total para todas as Licenças<br>36 (trinta e seis) meses** |
| 1 | 27502 | Serviços de fornecimento de subscrição de licenças de acesso à plataforma em nuvem de capacitação e conscientização em segurança da informação fornecida como serviço (SaaS), com implantação e suporte inclusos | Licença | 1.732 | **Cenário 1:** Média dos valores praticados nas últimas aquisições | **R$ 89,36** | **R$ 154.771,52** | **R$ 464.314.56** |
| | | | | | **Cenário 2:** Ser Órgão partícipe da aquisição que está em andamento no TRE-ES | **R$ 35,49** | **R$ 61.468,68** | **R$ 184.406,04** |

7.2. Resta evidente que a conveniência e oportunidade de buscar a participação na aquisição que está sendo realizada pelo TRE-ES podem alcançar economia recursos públicos que, em média, estima-se em aproximadamente 280 mil reais.

7.3. Alinhado com os princípios da administração pública da economicidade e da razoabilidade, recomendamos gestões para a participação no certame do TRE-ES como Órgão Partícipe da aquisição o que resultaria em um **valor estimado da contratação em R$ 184.406,04 (cento e oitenta e quatro mil quatrocentos e seis reais e quatro centavos).**

## 8 – DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

8.1 - Esta contratação é viável e necessária, considerando que:

8.1.1 - A necessidade da contratação encontra-se justificada no DOD Contratação TI DOD - STM/CJM 4234272.

8.1.2 - Os requisitos relevantes da contratação foram levantados e analisados.

8.1.3 -Os quantitativos e a escolha da solução estão fundamentados e alinhados às necessidades da Administração.

8.1.4 -Há recursos orçamentários disponíveis para suportar a contratação no corrente exercício financeiro.

8.1.5 -A equipe de planejamento da contratação declara que os elementos presentes nos estudos preliminares demonstram a VIABILIDADE da contratação pretendida.

8.1.6 -Que a solução pretendida mitiga riscos relacionados à segurança cibernética.

8.2 - Além das motivos supramencionados a viabilidade da solução pode ser comprovada considerando ainda os seguintes aspectos:

8.2.1 - Conforme já discorrido no item 3.3.2, dentre as soluções estudadas, aquela escolhida pelo TRE-ES, a plataforma Knowbe4, foi a única que Permite carga de treinamentos da contratante, incluindo os formatos de vídeo e SCORM (Moodle, plataforma de educação à distância utilizada na JMU - DIPES e ENAJUM).

8.2.2 - Destaca-se a aquisição pretendida pelo TRE-ES, visto que, conforme demonstrado nos itens 7.2 e 7.3, há oportunidade e conveniência desta Corte solicitar àquela Corte a possibilidade de ser Órgão partícipe da pretensa aquisição, em especial no que tange à economia de recursos públicos.

## 9 – INDICAÇÃO DA NECESSIDADE DE ADEQUAÇÃO AMBIENTAL

Plataforma em Nuvem - Não há necessidade de Adequação Ambiental

## 10 – APROVAÇÃO E ASSINATURA

| Equipe de Planejamento da Contratação | | |
|---|---|---|
| **INTEGRANTE DEMANDANTE** | **INTEGRANTE TÉCNICO** | **INTEGRANTE ADMINISTRATIVO** |
| **ALEXANDRE PASSOS DA COSTA**<br>Matrícula: 7625 | **EDUARDO BATISTA DOS SANTOS CORDEIRO**<br>Matrícula: 1183 | **LUIS GUSTAVO COSTA REIS**<br>Maticula: 7388 |

| AUTORIDADE MÁXIMA DA ÁREA DE TIC |
|---|
| **IANNE CARVALHO BARROS**<br>Diretor de Tecnologia da Informação e Transformação Digital<br>Matrícula: 7391 |

Documento assinado eletronicamente por **ALEXANDRE PASSOS DA COSTA**, **COORDENADOR DE SEGURANÇA CIBERNÉTICA**, em 17/03/2025, às 17:07 (horário de Brasília), conforme art. 1º,§ 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **LUIS GUSTAVO COSTA REIS**, **INTEGRANTE ADMINISTRATIVO**, em 17/03/2025, às 17:22 (horário de Brasília), conforme art. 1º,§ 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **EDUARDO BATISTA DOS SANTOS CORDEIRO**, **CHEFE DA SEÇÃO DE GESTÃO DE SEGURANÇA CIBERNÉTICA**, em 17/03/2025, às 18:31 (horário de Brasília), conforme art. 1º,§ 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **IANNE CARVALHO BARROS**, **DIRETOR DE TECNOLOGIA DA INFORMAÇÃO E TRANSFORMAÇÃO DIGITAL**, em 17/03/2025, às 23:37 (horário de Brasília), conforme art. 1º,§ 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.stm.jus.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **4234798** e o código CRC **4661D28F**.